ПРОФЕССИОНАЛИТЕТ, 2025, № 2 (006)

УДК *004.056.52*

А. А. Кязымов [1]***, А. А. Терешонок*** [1]

[1]*ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», , г. Москва, Российская Федерация*

ИНСТРУМЕНТЫ АВТОМАТИЧЕСКОЙ УСТАНОВКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ИНФРАСТРУКТУРЕ WINDOWS. ВОПРОСЫ БЕЗОПАСНОСТИ

Аннотация. *В данной статье проводится углубленный анализ безопасности встроенного механизма автоматической установки программного обеспечения Group Policy Software Installation (GPSI) в инфраструктуре Windows Active Directory. Исследование сосредоточено на практической оценке рисков, связанных с подменой установочных пакетов в сетевых хранилищах при небезопасной конфигурации прав доступа. В рамках экспериментальной работы развернута изолированная лабораторная среда, воспроизводящая типичный сегмент корпоративной доменной сети на базе Windows Server 2025 и Windows 10. Проведена серия атак, демонстрирующая, что при некорректной настройке разрешений NTFS — когда грунпе Authenticated Users предоставлены права на запись — злоумышленник с обычными привилегиями пользователя домена способен осуществить успешную подмену MSI-пакета и инициировать его установку на все рабочие станции домена. Установлено, что при отсутствии активированных политик проверки цифровых подписей клиентские системы не выполняют верификацию целостности и подлинности пакетов перед установкой, а стандартный аудит не фиксирует факт подмены файла. В рамках второй фазы эксперимента проведена валидация защитных мер: корректировка прав NTFS до уровня Read-only и активация политики обязательной проверки цифровых подписей эффективно блокируют описанный вектор атаки. Таким образом, основной риск обусловлен не архитектурными недостатками протокола, а ошибками конфигурирования и неиспользованием имеющихся механизмов защиты. На основе результатов исследования сформулированы конкретные практические рекомендации: строгий контроль доступа к сетевым хранилищам, применение подписанных MSI-пакетов и усиление аудита файловых операций в критичных ресурсах.*

Ключевые слова: *Group Policy, GPSI, безопасность Windows, автоматическая установка ПО, Active Directory, MSI, небезопасная конфигурация, подмена пакета, целостность.*

Введение

В данной статье представлен комплексный анализ, включающий теоретическое исследование выбранной темы, экспериментальную часть и детальное описание полученных результатов.

Механизм Group Policy Software Installation (GPSI) является стандартным и широко распространенным инструментом для централизованного развертывания программного обеспечения в доменных средах Windows. Его ключевые преимущества — тесная интеграция с Active Directory, отсутствие дополнительных лицензионных затрат и кажущаяся простота использования. Однако именно эта повсеместность и воспринимаемая надежность встроенного компонента операционной системы могут создавать ложное чувство безопасности. Процесс развертывания через GPSI предполагает размещение MSI-пакетов в общей сетевой папке, путь к которой указывается в объекте групповой политики. Данный архитектурный подход содержит фундаментальные риски, связанные с целостностью и конфиденциальностью канала распространения ПО, особенно при некорректной настройке прав доступа. Целью данного исследования является практическая демонстрация критических рисков, возникающих при небезопасной конфигурации GPSI, оценка эффективности стандартных защитных механизмов в конфигурации по умолчанию и разработка мер противодействия.

Анализ литературы и вопросы безопасности

Вопросы безопасности инфраструктуры Windows, в том числе связанные с групповыми политиками, освещаются в ряде научных и практических работ. Исследования Брысина А.Н., Журавлевой Ю.А., Котова И.Ю. [1], а также Корякина В.Ю. и Тищенко Э.В. [2] затрагивают базовые атаки и методы тестирования защиты доменной инфраструктуры, включая обход групповых политик. Однако специализированных глубоких исследований уязвимостей именно механизма GPSI, связанных с подменой пакетов на сетевом уровне, в доступных источниках недостаточно.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Работы Болотова А.С. и Болотовой Т.П. [3] посвящены файловой системе NTFS, что косвенно связано с настройкой разрешений для сетевых хранилищ ПО. Николаенкова О.А. и др. [4] рассматривают общие настройки безопасности Windows. Баранов А.Н. [5] анализирует повышение эффективности администрирования через групповые политики, но также без фокуса на рисках автоматической установки. Аспекты развертывания доменной инфраструктуры на базе Windows Server рассматриваются в работах Толганбаева Т.К. [7] и Николаева В.В. [6]. Вопросы организации киберполигонов для тестирования сетевой безопасности освещены Уйминым А.Г. [8]. В большинстве указанных работ основной акцент сделан на функциональность и администрирование, в то время как вопросы безопасности, такие как:

- отсутствие проверки целостности и подлинности (Integrity & Authenticity): GPSI не проверяет цифровые подписи, хэш-суммы или метки времени пакетов MSI;
- недостаточность модели контроля доступа (Access Control): стандартные разрешения на сетевых папках (например, Authenticated Users: Read) могут быть избыточны и не предотвращают несанкционированную запись;
- недостаточный аудит и мониторинг (Auditing & Monitoring): в журналах событий Windows отсутствуют специфические события, фиксирующие факт изменения установочного пакета после его публикации, остаются недостаточно проработанными. Данная статья призвана восполнить этот пробел, сфокусировавшись именно на практических аспектах реализации атак через небезопасную конфигурацию GPSI и мерах по их предотвращению.

Методология и экспериментальная установка

Для исследования была развернута изолированная лабораторная среда, воспроизводящая сегмент корпоративной сети:

- Контроллер домена — сервер на Windows Server 2025 с ролью Active Directory Domain Services.
- Клиентские рабочие станции — два компьютера под управлением Windows 10 Pro 22H2, введенные в домен.
- Сетевое хранилище — общая папка \\DC01\SoftwareDist на контроллере домена для размещения MSI-пакетов.
- Учетные записи — стандартная учётная запись пользователя домена (Hacker) с обычными привилегиями, имитирующая внутреннего нарушителя, и стандартная учётная запись (User) с обычными привилегиями.

Результат настройки на рисунке 1.

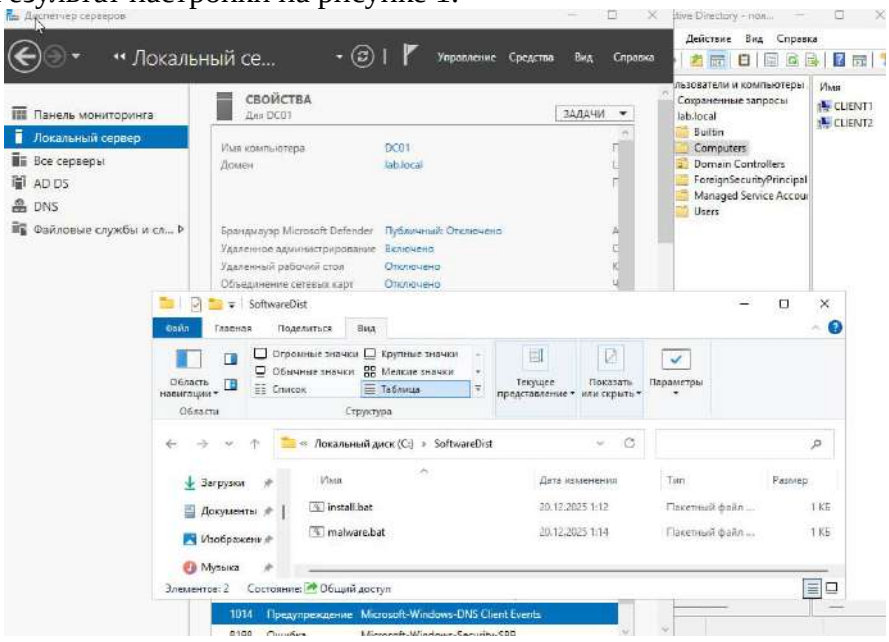

Рис. 1. Конфигурация изолированной лабораторной среды: контроллер домена DC01 (Windows Server 2025), клиентские рабочие станции WS01 и WS02 (Windows 10 Pro), сетевое хранилище \\DC01\SoftwareDist

Эксперимент и результаты

Фаза 1: Атака при небезопасной конфигурации.

Была произведена базовая настройка GPSI: создан MSI-пакет тестового приложения. В объекте групповой политики настроена установка программного обеспечения с указанием пути к пакету. Для имитации распространенной ошибки администрирования разрешения NTFS на сетевой папке были намеренно настроены некорректно: группе Authenticated Users предоставлены права Modify (включая запись и удаление). Установка легитимного пакета прошла успешно (Рисунки 2 и 3).

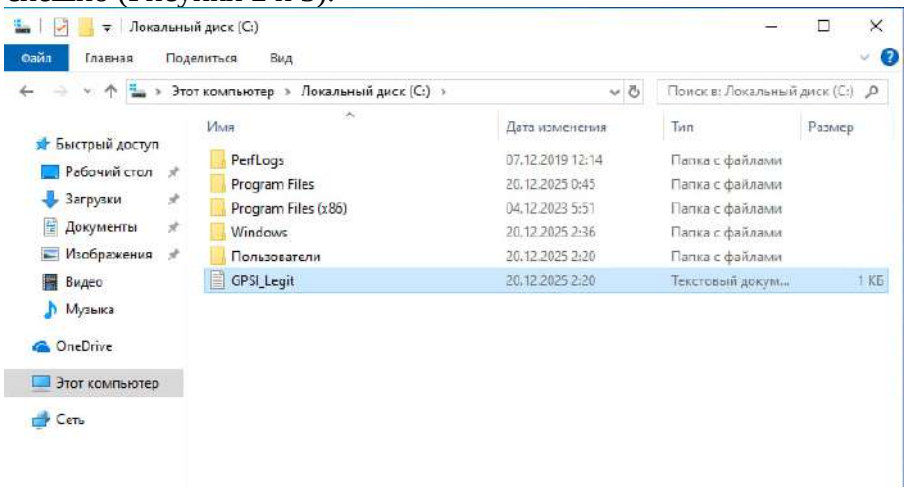

Рис. 2. Успешная установка легитимного MSI-пакета на клиентской рабочей станции до проведения атаки подмены

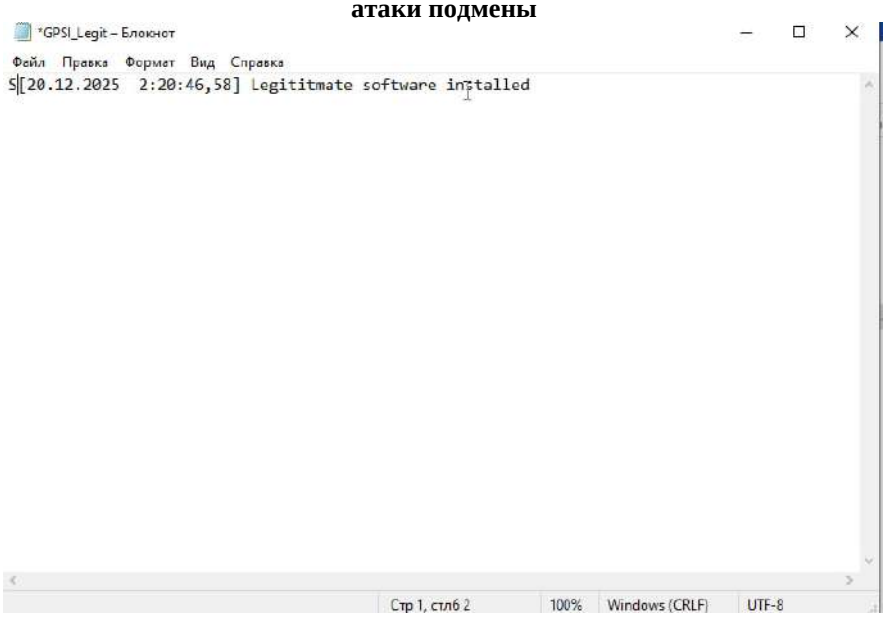

Рис. 3. Легитимный MSI-пакет в сетевой папке \\DC01\SoftwareDist с намеренно избыточными правами NTFS (Authenticated Users: Modify)

Злоумышленник (учетная запись Hacker) получает доступ к папке \\DC01\SoftwareDist и, пользуясь предоставленными правами Modify, заменяет легитимный MSI-пакет на вредоносный (в эксперименте — пакет, создающий текстовый файл-маркер) (Рисунок 4).

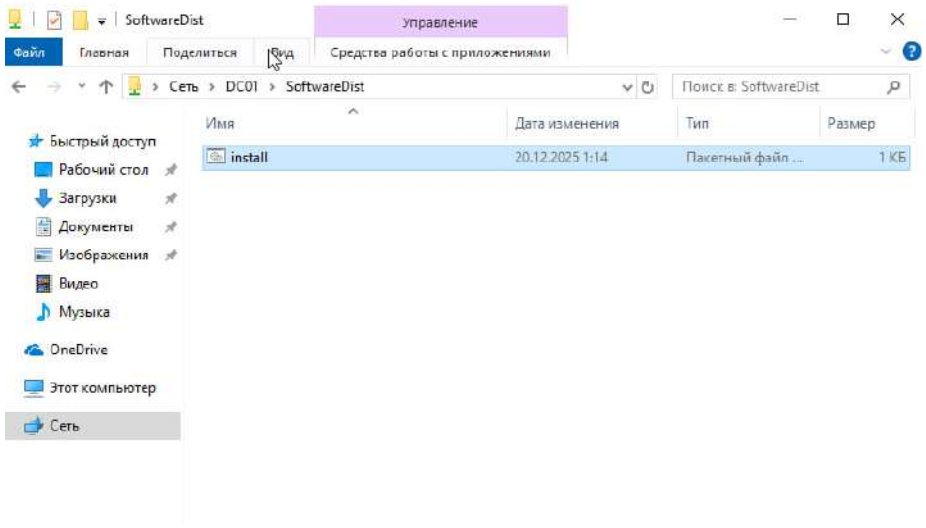

Рис. 4. Замена легитимного MSI-пакета вредоносным: учётная запись Hacker записывает подменный файл в сетевую папку, используя избыточные права Modify

После обновления групповых политик на клиентских компьютерах (автоматического или через gpupdate /force) был зафиксирован факт установки подмененного пакета на все рабочие станции в домене (Рисунок 5, 6).

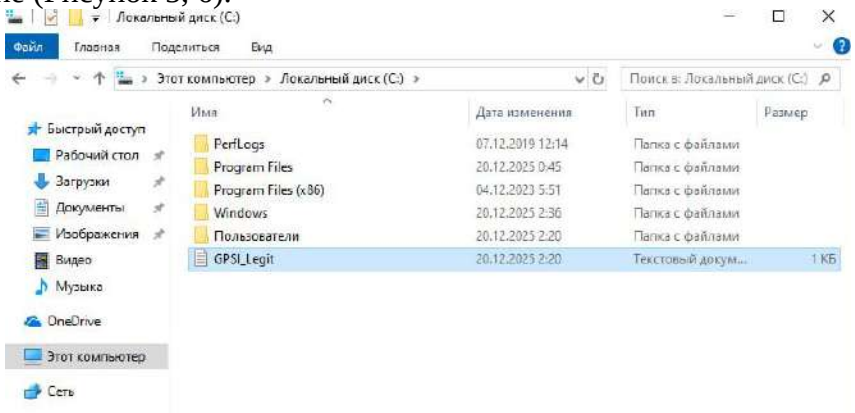

Рис. 5. Вредоносный MSI-пакет, размещённый учётной записью Hacker в сетевой папке вместо легитимного дистрибутива

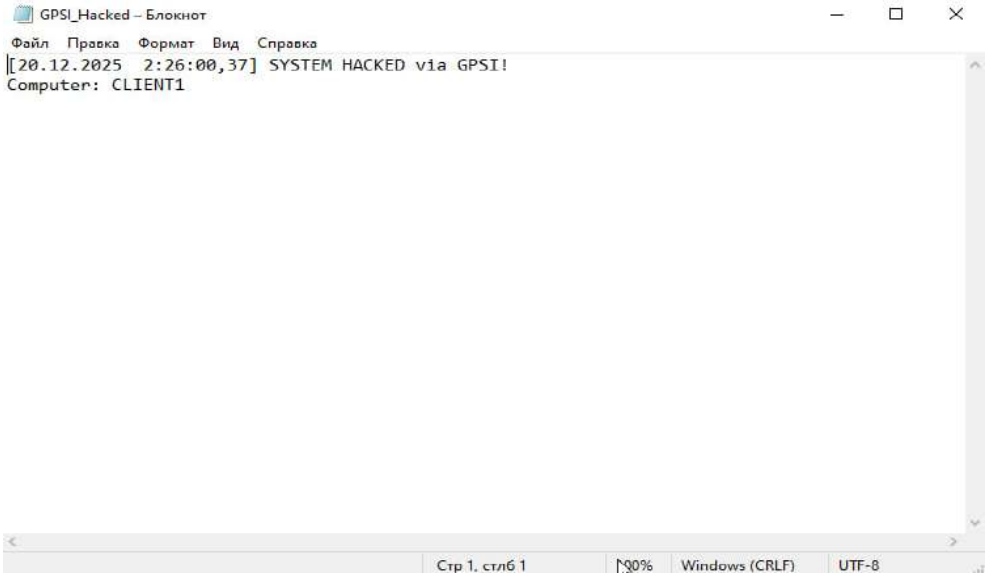

Рис. 6. Результат установки подменённого пакета на клиентской рабочей станции: создан файл-маркер, подтверждающий выполнение вредоносного кода

Эксперимент наглядно подтвердил критический риск, возникающий при небезопасной конфигурации прав доступа. Клиентские системы не выполнили никаких проверок цифровой подписи или целостности файла пакета перед установкой, так как соответствующие политики

не были активированы. Кроме того, была выявлена недостаточность стандартного аудита: в журналах событий отсутствовали явные записи о подмене пакета.

Количественные результаты Фазы 1:

В описанной небезопасной конфигурации атака была успешно воспроизведена; число независимых прогонов не фиксировалось.

Время до компрометации: от момента подмены пакета до установки на первый клиент — от нескольких минут (при принудительном обновлении политик) до 90 минут (стандартный интервал).

Фаза 2: Валидация мер защиты.

Для демонстрации эффективности контрмер был проведен дополнительный эксперимент. На той же лабораторной среде были последовательно применены и протестированы два защитных механизма:

Корректировка прав доступа: права NTFS для группы Authenticated Users на папке SoftwareDist были изменены на Read & Execute. Попытка учетной записи Hacker заменить или удалить MSI-пакет завершилась неудачей с ошибкой доступа. Атака была предотвращена на этапе доступа к хранилищу.

Включение проверки цифровых подписей: в политиках установщика Windows (Windows Installer) через Group Policy была активирована настройка "Запретить установку непроверенных пакетов" (параметр GPO: Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Установщик Windows → "Запрет установки пакетов без действительной цифровой подписи"). Попытка установки неподписанного (подмененного) пакета, даже при ошибочно оставленных правах на запись в сетевой папке, была заблокирована установщиком Windows с записью соответствующего сообщения об ошибке в журнале событий приложений.

Заключение

Таким образом, проведённое исследование продемонстрировало, что основной риск при использовании GPSI связан не с уязвимостью протокола как такового, а с небезопасной конфигурацией по умолчанию и потенциальными ошибками администрирования, такими как предоставление избыточных прав на запись в сетевое хранилище ПО. Хотя механизмы защиты (строгий контроль доступа NTFS и политики проверки цифровых подписей) существуют в платформе, они часто не используются, что делает инфраструктуру уязвимой для внутренних угроз.

Экспериментально подтверждено, что для минимизации рисков необходим комплексный подход:

1. Строгий контроль доступа: назначение на сетевые папки с установочными пакетами минимально необходимых прав (как правило, Read-only для рядовых пользователей и компьютеров).
2. Использование подписанных пакетов: внедрение практики подписи всех распространяемых MSI-пакетов цифровыми сертификатами и обязательное включение соответствующих политик проверки в домене.
3. Усиленный аудит и мониторинг: настройка аудита успешных и неуспешных попыток изменения файлов в критичных сетевых ресурсах для оперативного обнаружения инцидентов.

Применение этих мер, как показала вторая фаза эксперимента, эффективно блокирует описанный вектор атаки. Для критически важных инфраструктур также следует рассмотреть переход к более специализированным и безопасным по дизайну системам развертывания ПО.

Список литературы

1. Брысин А.Н., Журавлева Ю.А., Котов И.Ю. Исследование базовых атак и компрометации доменной Windows-инфраструктуры // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 2. – С. 45–53.
2. Корякин В.Ю., Тищенко Э.В. Тестирование защиты инфраструктуры GPO на базе Windows Server: анализ уязвимостей и методов обхода групповых политик // Труды

молодых ученых РГУ нефти и газа (НИУ) им. И.М. Губкина. – Москва : РГУ нефти и газа (НИУ) им. И.М. Губкина, 2025. – С. 1–10.
3. Болотов А.С., Болотова Т.П. Файловая система NTFS: обзор версий, производительность // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. – 2012. – № 3 (20). – С. 21–28.
4. Николаенкова О.А., Серик А.А., Хагуш Р.Э. Настройки конфигурации безопасности в Windows // Молодой исследователь Дона. – 2023. – № 1 (40). – С. 78–83.
5. Баранов А.Н. Повышение эффективности процессов администрирования компьютерных систем путем использования технологии групповых политик // Информационные технологии и системы : сб. науч. тр. – 2022. – С. 15–22.
6. Николаев В.В. Особенности реализации домена с тонкими клиентами на базе Microsoft Windows Server 2012 R2 // Международный студенческий научный вестник / СибАК. – Орёл. – 2016. – № 4. – С. 112–115.
7. Толганбаев Т.К. Доменные службы Active Directory и ядро сервера // Вестник магистратуры. – 2014. – № 11 (38). – С. 30–33. – ISSN 2223-4047.
8. Уймин А.Г. Нормирование показателей при организации киберполигона по сетевым технологиям // Нефть и газ – 2024 : тезисы докладов 78-й Международной молодежной научной конференции. – Москва : РГУ нефти и газа (НИУ) им. И.М. Губкина, 2024. – С. 1253–1254.

References

1. Brysin, A. N., Zhuravleva, Yu. A., & Kotov, I. Yu. (2023). Investigation of basic attacks and compromise of Windows domain infrastructure. Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii [Caspian Journal: Management and High Technologies], (2), 45–53.
2. Koryakin, V. Yu., & Tishchenko, E. V. (2025). Windows Server-based GPO infrastructure protection testing: Vulnerability analysis and methods of bypassing group policies. In Trudy molodykh uchenykh RGU nefti i gaza (NIU) im. I.M. Gubkina [Proceedings of Young Scientists of Gubkin University] (pp. 1–10). Gubkin Russian State University of Oil and Gas (NIU).
3. Bolotov, A. S., & Bolotova, T. P. (2012). The NTFS file system: Version overview and performance. Vestnik Tomskogo gosudarstvennogo universiteta. Upravleniye, vychislitelnaya tekhnika i informatika [Tomsk State University Journal of Control and Computer Science], (3), 21–28.
4. Nikolaenkova, O. A., Serik, A. A., & Hagush, R. E. (2023). Security configuration settings in Windows. Molodoy issledovatel Dona [Young Researcher of the Don], (1), 78–83.
5. Baranov, A. N. (2022). Improving the efficiency of computer system administration processes through the use of group policy technology. In Informatsionnyye tekhnologii i sistemy: sbornik nauchnykh trudov [Information Technologies and Systems: Collected Papers] (pp. 15–22).
6. Nikolaev, V. V. (2016). Features of implementing a domain with thin clients based on Microsoft Windows Server 2012 R2. Mezhdunarodnyy studencheskiy nauchnyy vestnik [International Student Scientific Bulletin], (4), 112–115.
7. Tolganbaev, T. K. (2014). Active Directory domain services and the server core. Vestnik magistratury [Bulletin of the Magistracy], (11), 30–33. ISSN 2223-4047.
8. Uymin, A. G. (2024). Normalization of indicators in the organization of a cyber range on network technologies. In Neft i gaz – 2024: Tezisy dokladov 78-y Mezhdunarodnoy molodezhnoy nauchnoy konferentsii [Oil and Gas – 2024: Abstracts of the 78th International Youth Scientific Conference] (pp. 1253–1254). Gubkin Russian State University of Oil and Gas (NIU).

Информация об авторах

Кязымов Адалат Адалатович — студент факультета комплексной безопасности ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: adalat.kiazymov@mail.ru

Терешонок Артём Алексеевич — студент факультета комплексной безопасности ТЭК, ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: kr3nver@yandex.ru

AUTOMATED SOFTWARE DEPLOYMENT TOOLS IN WINDOWS INFRASTRUCTURE. SECURITY ISSUES

Kyazimov A. A.[1], Tereshonok A. A.[1]

[1]National University of Oil and Gas «Gubkin University»

Abstract. *This article presents an in-depth security analysis of the built-in Group Policy Software Installation (GPSI) mechanism used for centralized software deployment in Windows Active Directory environments. The research focuses on the practical assessment of security risks associated with the substitution of MSI installation packages stored in network shares under misconfigured access permissions. An isolated laboratory environment was deployed to simulate a typical corporate domain network segment, comprising a Windows Server 2025 domain controller and two Windows 10 Pro client workstations. A series of attack scenarios was conducted, demonstrating that when NTFS permissions are incorrectly configured — specifically, when the Authenticated Users group is granted Modify rights — a low-privileged domain user can successfully replace a legitimate MSI package with a malicious one and trigger its installation on all domain workstations. It was established that, in the absence of activated digital signature verification policies, client systems perform no integrity or authenticity checks on packages prior to installation, and standard event logging does not capture file substitution events. A second experimental phase validated two countermeasures: restricting NTFS permissions to Read-only and enabling mandatory digital signature verification policies. Both measures effectively blocked the described attack vector. The findings indicate that the primary risk stems not from architectural flaws in the GPSI protocol itself, but from configuration errors and the non-utilization of available platform-level security controls. Practical recommendations are formulated covering strict access control, mandatory MSI package signing, and enhanced file auditing on critical network shares.*

Keywords: *Group Policy, GPSI, Windows security, automatic software installation, Active Directory, MSI, vulnerabilities, package substitution, integrity, audit.*

Information about the authors

Kyazimov Adalat Adalatovich — student of the Faculty of Integrated Fuel and Energy Complex Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: adalat.kiazymov@mail.ru

Tereshonok Artem Alekseevich — student of the Faculty of Integrated Fuel and Energy Complex Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: kr3nver@yandex.ru